In the Abstract:

ABSTRACT OF THE DISCLOSURE

In an electronic voting process, a voter ($\mathbf{V_i}$) encrypts his vote (v_i) according to the encryption scheme ($\mathbf{E_{TM}}$) of a tallier mix-net (50) used to tally up the votes cast. The voter ($\mathbf{V_i}$) obtains on his encrypted vote, (x_i), from an admin server module (20), a digital signature according to a fair blind signature scheme (**FBSS**). The encrypted vote (x_i) is encrypted a second time, together with the unblinded digital signature (y_i) thereof by the admin server, using the encryption scheme ($\mathbf{E_M}$) of a randomizing mix-net (40), to yield an output (c_i), and the voter uses his own signature scheme (S_i) to sign this, giving (σ_i). The voter sends an ID code and data including (c_i, σ_i) to a bulletin board server (30). Discrepancies in this vote data can be detected and their origin traced by prompting the randomizing mix-net servers (40) to provide proofs of correctness, and using the signature-tracing mechanism of FBSS.

~~(Fig.1)~~